Docket No.

242895US2SRD

#### IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF:

Hideo SHIMIZU, et al.

SERIAL NO: NEW APPLICATION

GAU:

FILED:

HEREWITH

**EXAMINER:** 

FOR:

POLYNOMIAL INVERSE COMPUTING APPARATUS, MULTIPLIER APPARATUS AND POLYNOMIAL

**INVERSE COMPUTING METHOD** 

## INFORMATION DISCLOSURE STATEMENT UNDER 37 CFR 1.97

COMMISSIONER FOR PATENTS ALEXANDRIA, VIRGINIA 22313

SIR:

Applicant(s) wish to disclose the following information.

#### REFERENCES

- The applicant(s) wish to make of record the references listed on the attached form PTO-1449. Copies of the listed references are attached, where required, as are either statements of relevancy or any readily available English translations of pertinent portions of any non-English language references.
- ☐ A check is attached in the amount required under 37 CFR §1.17(p).

#### RELATED CASES

- ☐ Attached is a list of applicant's pending application(s) or issued patent(s) which may be related to the present application. A copy of the patent(s), together with a copy of the claims and drawings of the pending application(s) is attached along with PTO 1449.
- A check is attached in the amount required under 37 CFR §1.17(p).

### CERTIFICATION

- ☐ Each item of information contained in this information disclosure statement was first cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this statement.
- ☐ No item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application or, to the knowledge of the undersigned, having made reasonable inquiry, was known to any individual designated in 37 CFR §1.56(c) more than three months prior to the filing of this statement.

### DEPOSIT ACCOUNT

Please charge any additional fees for the papers being filed herewith and for which no check or credit card payment form is enclosed herewith, or credit any overpayment to deposit account number 15-0030. A duplicate copy of this sheet is enclosed.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND, MAIER & NEUSTADT, P.C.

Marvin J. Spivak

Registration No. 24,913

C. Irvin McClelland Registration Number 21,124

Customer Number

22850

Tel. (703) 413-3000 Fax. (703) 413-2220 (OSMMN 05/03)

DOCKET NO: 242895US2SRD Sheet <u>1</u> of <u>1</u>

IN RE APPLICATION OF: Hideo SHIMIZU, et al.

SERIAL NO: New Application

FILED: Herewith

FOR: POLYNOMIAL INVERSE COMPUTING APPARATUS, MULTIPLIER APPARATUS

AND POLYNOMIAL INVERSE COMPUTING METHOD

## **STATEMENT OF RELEVANCY**

## Reference AO (JP 2000-47833) on Form PTO- 1449:

This publication is referred to in the specification. See page 3, line 5.

# Reference AP (JP 2000-315201) on Form PTO- 1449:

This publication is referred to in the specification. See page 3, line 6.

# Reference AQ (JP 2000-322280) on Form PTO- 1449:

This publication is referred to in the specification. See page 3, line 7.

## Reference AR (JP 2002-23999) on Form PTO- 1449:

This publication is referred to in the specification. See page 3, line 8.

### Reference AW on Form PTO- 1449:

This paper describes another algorithm the named "almost inverse algorithm" with same purpose. It use quite different technique from my invention.

# Reference AX on Form PTO- 1449:

This book describes known several algorithms for calculating modular inverse in GF (2<sup>m</sup>)

Form PTO 1449		U.S. DEPARTMENT	OF COMMERCE	ATTY DOCKET NO.		SERIAL NO. NEW APPLICATION		
(Modified)		PATENT AND TRAD	EMARK OFFICE	242895US2SRD				
				APPLICANT				
LIST OF	REFER	RENCES CITED BY AP	PLICANT	Hideo SHIMIZU, et al.				
				FILING DATE		GROUP		
				HEREWITH				
U.S. PATENT DOCUMENTS								
EXAMINER		DOCUMENT	DATE	NAME	01.460	SC SUB FILING DATE		
INITIAL		NUMBER	DATE	NAME	CLASS	CLASS	IF APPROPRIATE	
	AA							
	AB							
	AC							
	AD							
	AE							
	AF							
	AG							
	AH							
	ΑI							
	AJ	•				i		
	AK							
	AL							
	AM							
	AN		<u> </u>					
		<u> </u>	FC	REIGN PATENT DOCUMENTS				-
		DOCUMENT NUMBER	DATE	COUNTRY		YES		ATION NO
	AO	2000-47833	02/18/00	Japan				x
	AP	2000-315201	11/14/00	Japan				×
	- AO	2000-322280	11/24/00	Japan				×
	AR	2002-23999	01/25/02	Japan				×
	AS							
	AT							
	ΑU							
	AV							
OTHER REFERENCES (Including Author, Title, Date, Pertinent Pages, etc.)								
	R. SCHROEPPEL, et al., "Fast Key Exchange with Elliptic Curve Systems", CRYPTO '95, LNCS 963, 1995, pgs. 43-56							
	AX	A. J. MENEZES, et al., "Handbook of Applied Cryptography", CRC PRESS, 1997, pgs.591-634						
	AY							
	AZ				Additional References sheet(s) attached			
Examiner					Date Considered			
*Examiner: Initial if reference is considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.								